Description of Actual State Sensor Types for the Vulnerability Management (VULN) Capability

30 Jul 2014

1 Purpose

This document is intended to provide insight on the types of tools and technologies that can be utilized to support the collection of vulnerability information required to perform the Continuous Diagnostics and Mitigation (CDM) VULN capability. The 'Description of Generic Sensor Types for the Continuous Diagnostic and Mitigation (CDM) Collection System' document describes the Actual State generic sensor types for CDM to include information about potential for operational impacts and general data accuracy issues associated with each particular sensor type.

The VULN capability ensures that software with known vulnerabilities is identified and either remediated or removed or from devices to minimize exploitation. The VULN capability can use data collected by the Software Asset Management (SWAM) and Configuration Settings Management (CSM) Actual State sensors to identify software products with known vulnerabilities that are not mitigated by current configuration settings. Essentially, the VULN capability requires the same actual state data as the SWAM and CSM capabilities. That data is then compared to a different desired state specification: a listing of software that has at least one known vulnerability and any configuration settings that effectively mitigate a particular vulnerability.

There are active network sensors and endpoint-based agents that specialize in vulnerability discovery (e.g., vulnerability scanners) and many are widely deployed across most D/A environments. If these types of products are used, their output must be converted to report the vulnerable software, and not the CVEs, that are present. For example, if a particular executable has a CVE associated with it and that executable is associated with three distinct software products, then the actual state information that must be collected is the presence of any or all of the three distinct products not the presence of the one vulnerability.